Breaking a Recent SoC's Hardware AES Accelerator Using Body Biasing Injection

Karim M. Abdellatif, PhD

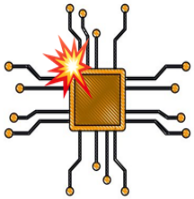
Motivation

- Several security devices have been deployed in the market
- Hardware security evaluation is **"must"**
- Being updated with new/recent attack techniques is **important**

Source: bitcoinmagazine.com

FAULT ATTACKS

- Perturbing the chip during sensitive operations
  - Secure boot [1]
  - Cryptographic operations (AES, DES, RSA, ...) [2]

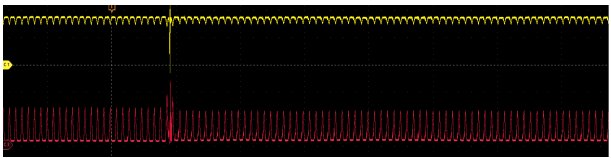


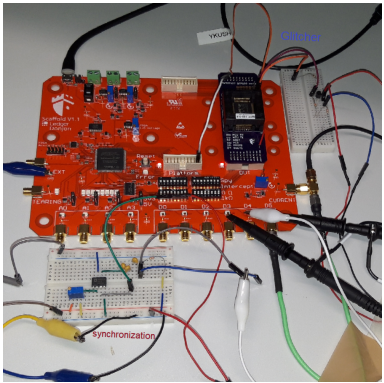
[1] Albert Spruyt and Niek Timmers, "Bypassing Secure Boot Using Fault Injection", Black Hat Europe 2016.

[2] Yifan Lu, "Attacking Hardware AES of PlayStation with DFA", 2019

Power Glitches

- The main idea is to drop the VDD of the chip for a short time (ns) during the sensitive operation
- This can be done using a MOSFET
- A challenge when the chip has different VDD sources
- It doesn't need any chip decapping



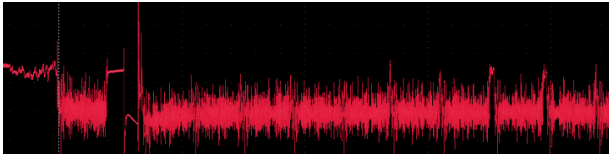


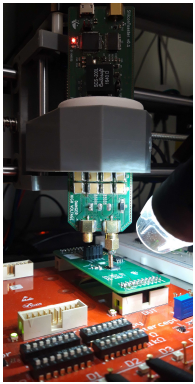
Glitch Setup [3]

[3] Karim Abdellatif and Olivier Hériveaux , "Keep it Cheap: Multiple Faults Attacks in Practice", JAIF 2020.

EMFI

- Injecting electromagnetic field into the chip to create perturbations
- High voltage pulse is injected to the probe to create EMFI
- It may need decapping the chip (packaging thickness)



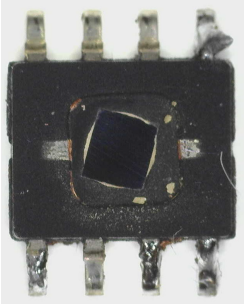


EM Setup [4]

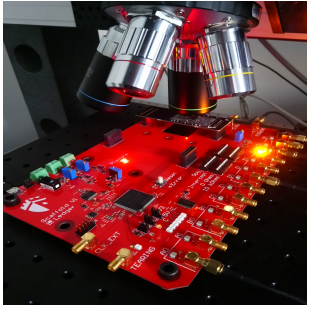
[4] Karim Abdellatif and Olivier Hériveaux , "SiliconToaster: A Cheap and Programmable EM Injector for Extracting Secrets", FDTC 2020.

Laser Attack

- It needs decapping the chip
- The laser energy will induce a current into transistors
- The induced current can temporarily invert the output of a logic cell, thus possibly generating an error in the circuit
- Expensive setup



Decapped chip [5]



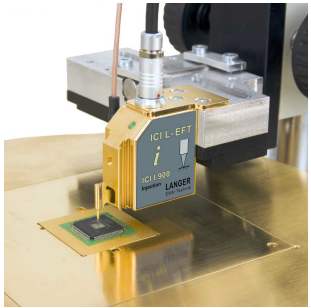
Laser Setup [5]

[5] Olivier Hériveaux , "Black-box Laser Fault Injection on a Secure Memory", SSTIC 2020.

BODY BIASING INJECTION (BBI)

Body Biasing Injection

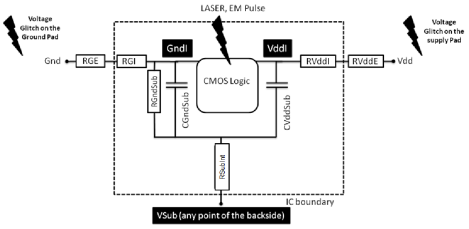
- It was proposed by P. Maurine [6]
- The main idea of BBI is to apply a voltage pulse onto the backside of the integrated circuit die by using a needle
- It needs decapping the chip
- It generates a localized ground glitching.



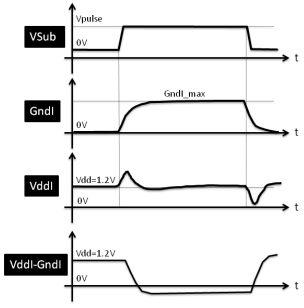
Source: Langer

[6] P. Maurine, K. Tobich, T. Ordas, and P. Liardet, "Yet Another Fault Injection Technique:by Forward Body Biasing Injection", YACC, 2012.

Body Biasing Injection

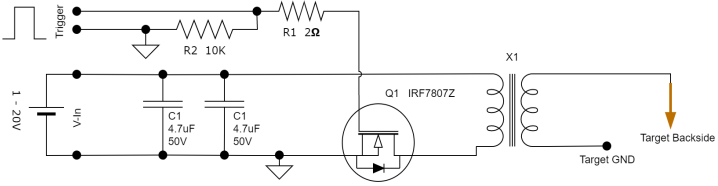


Power/ Ground Network of an IC as shown in [6]

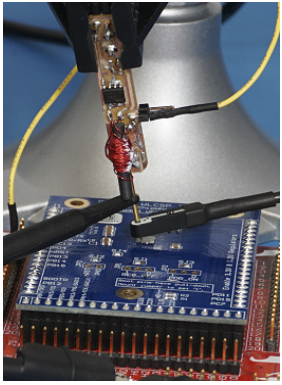


Simulated BBI effect as shown in [8]

[6] P. Maurine, K. Tobich, T. Ordas, and P. Liardet, "Yet Another Fault Injection Technique:by Forward Body Biasing Injection", YACC, 2012.



Low-cost BBI Injector shown in [7]

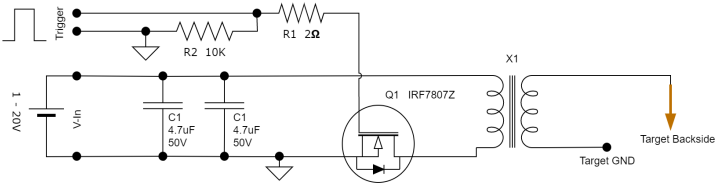


BBI setup shown in [7]

[7] Colin O'Flynn, "Low-Cost Body Biasing Injection (BBI) Attacks on WLCSP Devices", CARDIS 2020.

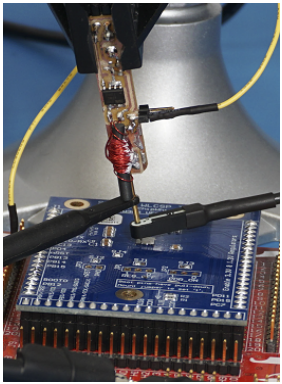
HOMEMADE BBI SETUP

Improving CARDIS 2020



Low-cost BBI Injector shown in [7]

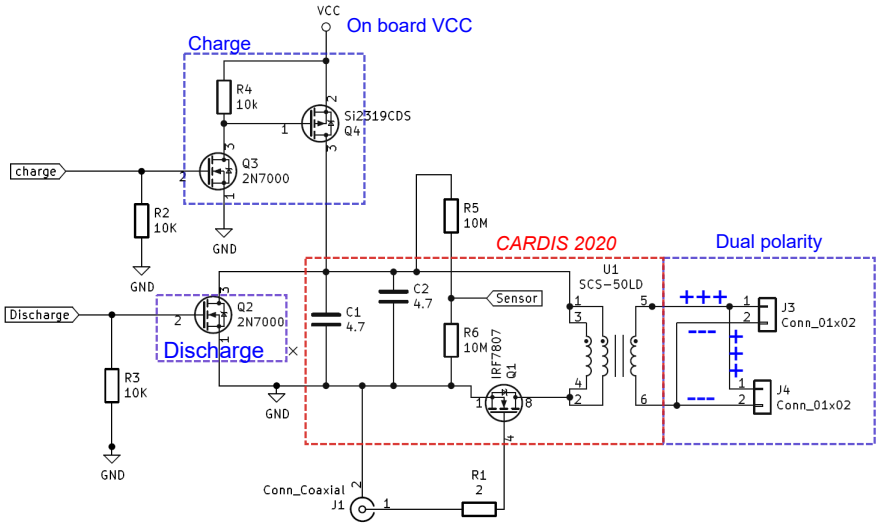
Pulse Polarity + External power supply



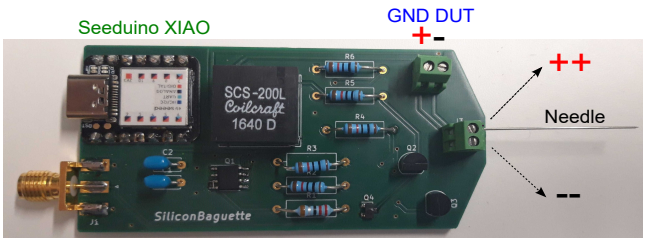
BBI setup shown in [7]

[7] Colin O'Flynn, "Low-Cost Body Biasing Injection (BBI) Attacks on WLCSP Devices", CARDIS 2020.

Homemade BBI injector

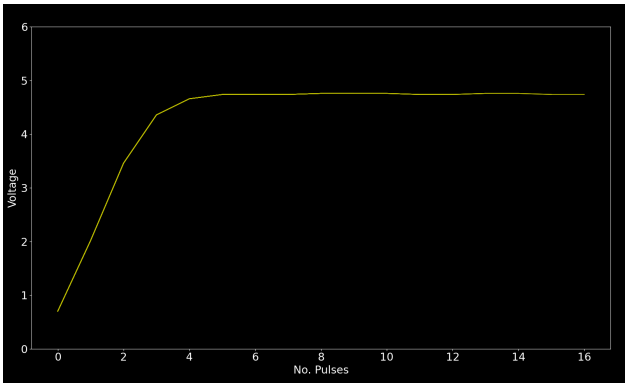


Homemade BBI injector: SiliconBaguette



- The MCU is used to control charging/discharging the capacitors (**Programmability up to 250V**)
- Positive and negative voltage pulses (**Dual polarity**)
- Credits for soldering small components and PCB support goes to Olivier Hériveaux

Homemade injector: Programmable voltage pulse



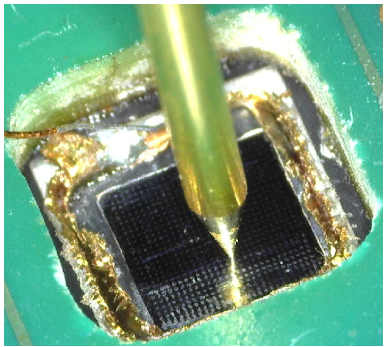
- Transformer Turns Ratio = 1:50
- Max Voltage = 5 x 50 = 250V

DUT

- A low-cost and low-power system on chip (SoC)
- It is a single 2.4 GHz Wi-Fi-and-Bluetooth chip designed with the TSMC 40 nm technology
- Recently, it has been deployed in a hardware wallet as the main MCU

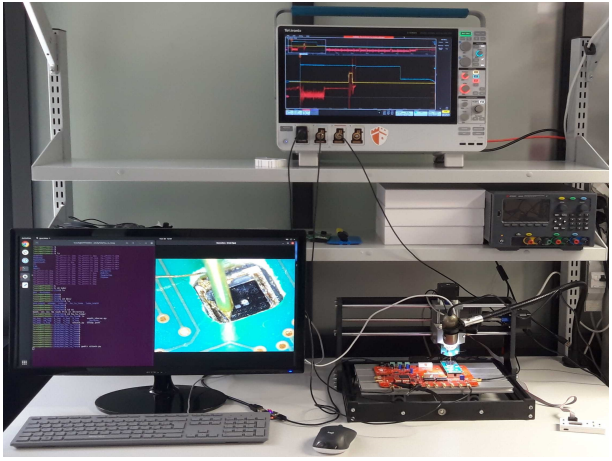
Validation

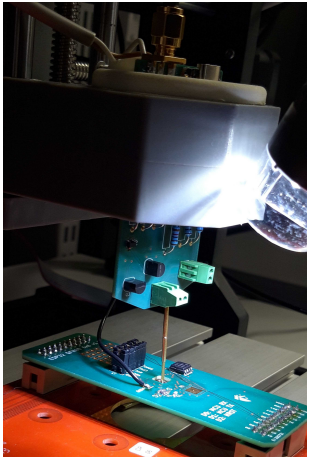
```
digitalWrite(4, HIGH); //Trigger High
for (int i = 0; i < 500; i++)
{
    i++;
}
digitalWrite(4, LOW); //Trigger Low
Serial.print(i);
if(i != 500)
{
    Serial.print("Faulted");
}
else
{
    Serial.print("Ok");
}
```



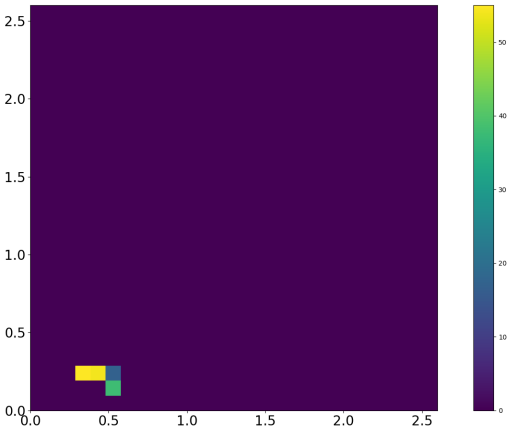
Running the glitchable application + Scanning the overall chip surface + Dual polarity

Setup

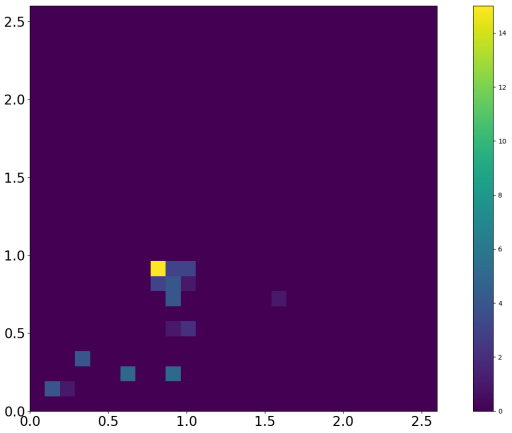




Successful faults

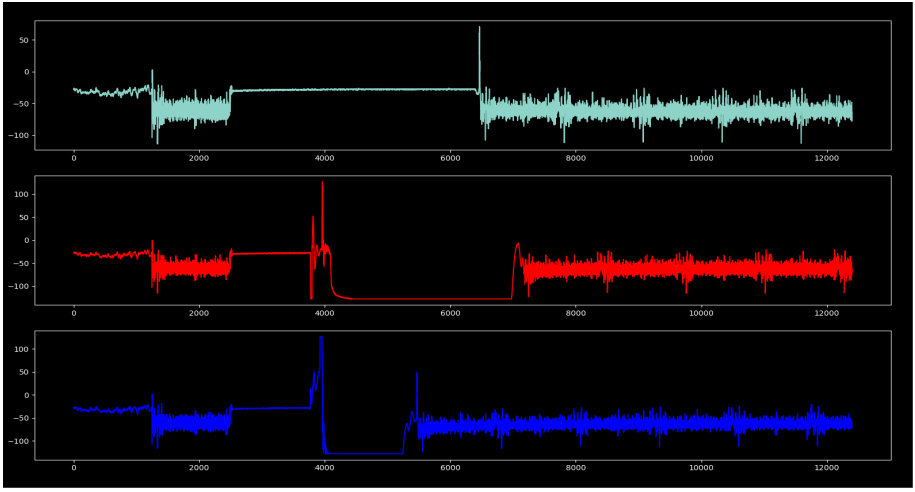


Positive pulse



Negative pulse

Polarity difference



No Fault

Positive

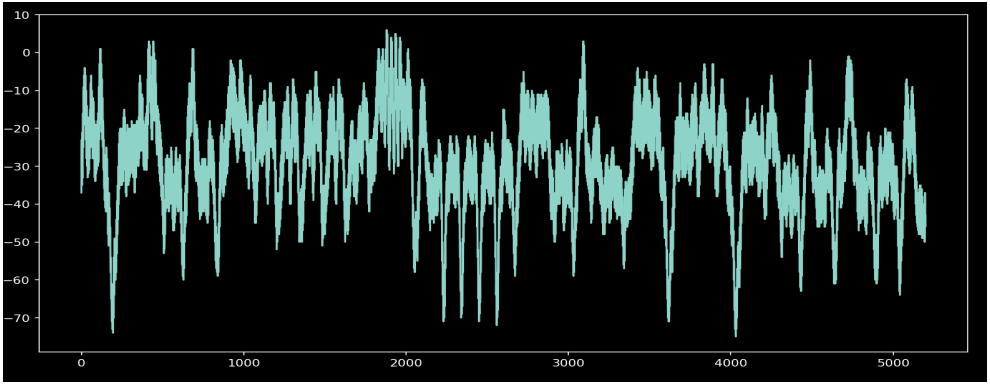
Negative

BREAKING HW AES

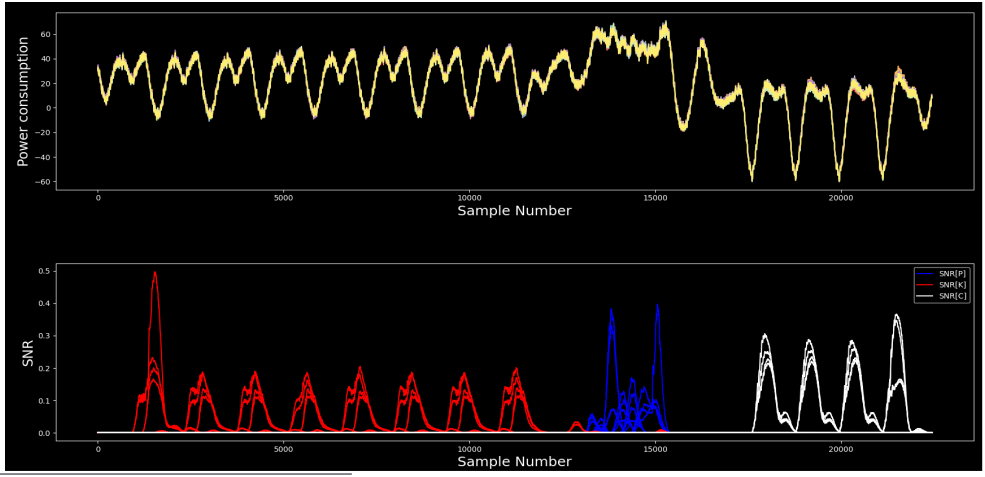
DUT's HW AES

- The DUT has cryptographic hardware accelerators: AES, SHA-2, RSA, Elliptic Curve Cryptography (ECC), Random Number Generator (RNG)
- AES-128 was selected as an evaluation target using BBI

HW AES-128

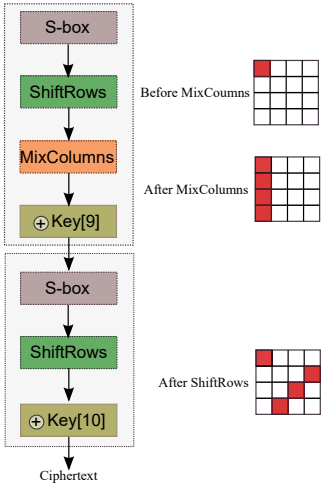


Leakage detection [8]



[8] S. Bhasin, J. Danger, S. Guilley, Z. Najm, "NICV: Normalized Inter-Class Variance for Detection of Side-Channel Leakage", IACR 2013

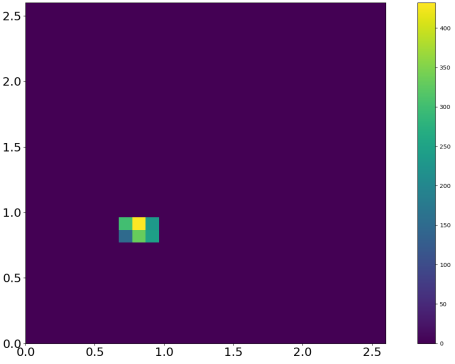
Differential Fault Analysis [9]



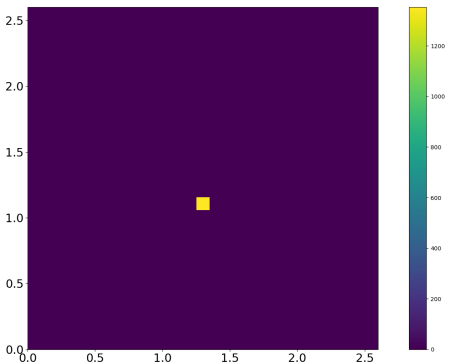
- Two faults are needed for each column to attack the overall key of AES-128

[9] P. Dusart, G. Letourneux, O. Vivolo, "Differential fault analysis on AES", 2003.

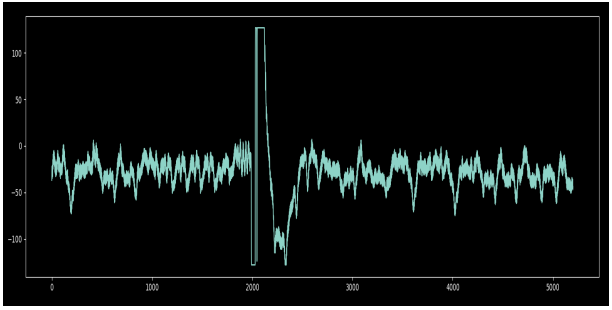
Fault Analysis



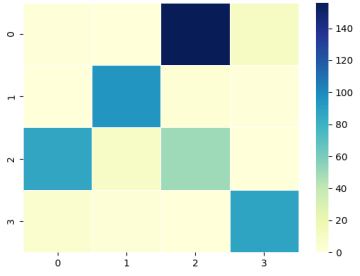
Faulting the communication of Ciphertexts using 250V



Faulting the AES using 500V (external power supply)



Faulted AES power consumption



Single byte faults in round 9 of the AES after 10K iterations

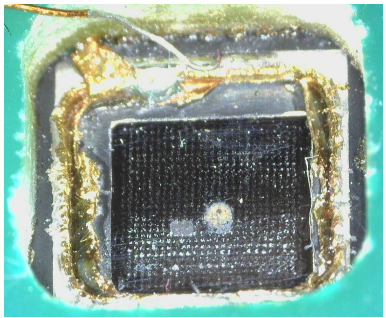
Obtained faults in round 9 are sufficient to extract the overall key of the AES-128.

[9] P. Dusart, G. Letourneux, O. Vivolo, "Differential fault analysis on AES", 2003.

NOTES

Side notes

- Be careful during decapping the chip
- High voltages may damage the chip (I damaged 3 chips)
- Avoid moving the needle (X and Y), while it is in fully touch with the chip



Post experiment

CONCLUSION

Conclusion and Future work

- A cheap (and compact) setup for BBI was presented
- Breaking the HW AES of a recent SoC in few hours (10K trials)
- The SiliconBaguette will be released in few days on GitHub
- Future work
  - Evaluating more SoCs
  - Studying the effect of BBI on fault detectors (ex: glitch detectors)

THANK YOU. QUESTIONS?

Karim M. Abdellatif, PhD
e-mail: karim.abdellatif@ledger.fr